VZCZCXRO5719
PP RUEHAG RUEHAO RUEHAP RUEHAST RUEHAT RUEHBC RUEHBI RUEHBL RUEHBZ
RUEHCD RUEHCHI RUEHCI RUEHCN RUEHDA RUEHDBU RUEHDE RUEHDF RUEHDH
RUEHDT RUEHDU RUEHED RUEHEL RUEHFK RUEHFL RUEHGA RUEHGD RUEHGH RUEHGI
RUEHGR RUEHHA RUEHHM RUEHHO RUEHHT RUEHIHL RUEHIK RUEHJS RUEHKN RUEHKR
RUEHKSO RUEHKUK RUEHKW RUEHLA RUEHLH RUEHLN RUEHLZ RUEHMA RUEHMC
RUEHMJ RUEHMR RUEHMRE RUEHMT RUEHNAG RUEHNG RUEHNH RUEHNL RUEHNP
RUEHNZ RUEHPA RUEHPB RUEHPD RUEHPOD RUEHPT RUEHPW RUEHQU RUEHRD RUEHRG
RUEHRN RUEHROV RUEHRS RUEHSK RUEHTM RUEHTRO RUEHVC RUEHVK RUEHYG
DE RUEHC #4974 1241517
ZNR UUUUU ZZH
P 041458Z MAY 09

FM SECSTATE WASHDC

TO ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE PRIORITY
RUEHTRO/AMEMBASSY TRIPOLI PRIORITY 7100

UNCLAS STATE 044974

FOR IMO; ALSO FOR RIMC

E.O. 12958: N/A
TAGS: AADP ACOA AMGT KRIM

SUBJECT: DEFENSE CONNECT ONLINE (DCO) IMPLEMENTATION

¶1. Information Resource Management (IRM) has collaborated with the Department of Defense (DoD) to evaluate the use of the Defense Connect Online (DCO) collaboration suite on OpenNet. After sufficient review, the necessary configuration changes and security controls have been evaluated and approved to allow the use of DCO on OpenNet.

¶2. Enterprise Network Management (IRM/OPS/ENM), Information Assurance (IRM/IA) and the Office of Computer Security (DS/SI/CS) have made a coordinated effort to evaluate and test the required settings on OpenNet workstations. The team found that the current Windows XP configuration complied with most, but not all settings required by DCO.

¶3. To provide control over the configuration change supporting DCO, local administrators have at least two options: 1) Visit the workstations individually to make the change in the mms configuration file; 2) Create a Group Policy Object (GPO) that they administer locally to apply this change to the chosen workstation. The specific OpenNet workstation setting to be changed is listed below.

Edit the C:\WINDOWS\system32\Macromed\Flash\mms.cfg file and change "AVHardwareDisabled = 1" setting to "AVHardwareDisabled = 0".

This change enables voice capability for DCO collaboration sessions.

¶4. IRM/IA and DS/SI/CS have determined that the following security controls are needed for workstations using the DCO suite.
- Defense Connect Online is authorized (1) outside the CAA or (2) in Dedicated Unclassified Space approved by the RSO/SEO if inside the CAA. (See 12 FAH-6 H-542.5-5)

- The Adobe Flash Player 9.0.124 that is currently approved for Department use is susceptible to security vulnerabilities that could exploit cameras and microphones attached to Department computers. Proper vigilance and security awareness by individuals using the collaboration tool is essential.

- Use of cameras or microphones attached to specific computers on OpenNet must be for mission critical business requirements only.

- The microphone and camera installed on a workstation in support of a collaboration session must be disconnected when not in use. It is recommended that the microphone and camera be installed on the workstation just prior to the DCO session and removed immediately upon completion of the session.

- Managers at locations where the microphone and camera features within Adobe are enabled must ensure users are properly trained on the best security practices for their use.

¶5. Questions about information system security issues and the use of DCO should be sent to ASKCS@state.gov.

¶6. Minimize considered.
CLINTON